AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions of claims in the application.

LISTING OF THE CLAMS:

Claim 1 (Currently Amended): In quantum cipher communication using a light signal, a quantum cipher communication system characterized in that:

it uses a phase difference between a weak signal light which is so weak that a change in its quantum mechanical state is detectable and an intense ~~a~~ reference light ~~which have orthogonal polarizations~~ for communicating a ~~signal of~~ privacy key, wherein said phase difference is produced by a sender and a recipient adding a phase on the signal light or the reference light;

it has an optical balanced homodyne detector which detects said phase difference as a difference signal of the detector,

wherein ~~the~~ said phase difference is ~~determined~~ assigned to bit 0 or bit 1 by comparing said difference signal with ~~a~~ threshold values which are determined from a quantum-mechanical probability distribution of said difference signals obtained from a set of said phase differences assigned bit 0 or bit 1; and

wherein an eavesdropping is detected by the recipient measuring a change in ~~a~~ said quantum-mechanical probability distribution of said difference signal, which is produced by the eavesdropping operation.

Claim 2-14 (Canceled):

Claim 15 (Currently Amended): In quantum cipher communication using a light signal, a quantum cipher communication system ~~having~~ as set forth in claim 1, which comprises a sender's apparatus, a recipient's apparatus and a transmission path connecting between the sender's apparatus and the recipient's apparatus, and is characterized in that

the sender's apparatus comprises of:

a light source for a laser beam;

a beam splitting means for splitting said laser beam into a signal light and a reference light;

a phase modulation means making a phase change for every light which is either of said signal light or said reference light; and

a light attenuation means for attenuating said signal light intensity,

the recipient's apparatus comprises of:

a phase modulation means making a phase change for every light which is either of said signal light or said reference light transmitted from the sender's apparatus through the transmission path;

a superimposing means for superimposing said signal light and said reference light, either of which is phase changed by said phase modulation means of the recipient's apparatus;

a pair of ~~photo-detector~~ photoconductive diodes for converting two output lights from said superimposing means into respective electric signals; and

an amplifying means for amplifying a difference signal between said electric signals,

wherein the sender, by using said phase modulation means of sender's apparatus, imparts for every light a phase change randomly selected from a set of phase changes predetermined by the sender and the recipient, and the recipient, by using said phase modulation means of recipient's apparatus, imparts for every light a phase change randomly selected from said set of phase changes, as well as measures for every light said difference signal between the electric signals amplified by the amplifying means;

then, by using a public communication line, the recipient notifies to the sender said phase changes imparted by the recipient for every light;

the sender calculates ~~the~~ a total phase difference between ~~the~~ said signal light and ~~the~~ said reference light by adding the phase change ~~notified~~ made by the recipient and the phase change ~~imparted~~ made by the sender for every light, and notifies to the recipient each of the lights whose total phase difference satisfy a total phase condition predetermined by the sender and the recipient, as a raw key ~~for~~ candidate for being adopted as a privacy key;

then the recipient, for said every light notified as a raw key ~~for~~ candidate, assigns bit 1 when said difference signal measured is equal or greater than a ~~predetermined~~ threshold value

+X, and assigns bit 0 when said difference signal measured is equal or less than ~~the~~ a ~~predetermined~~ threshold value - X, whereby the recipient gets a privacy key;

the sender, for said every light ~~making~~ notified as a raw key ~~for~~ candidate, assigns bit 1 or 0 according to a condition regarding the total phase difference, which is predetermined by the sender and the recipient, whereby the sender gets a privacy key;

wherein said threshold values +X and - X are determined from said quantum-mechanical probability distribution;

wherein an eavesdropping is detected by said recipient measuring a change in a quantum-mechanical probability distribution; and

wherein the sender and the recipient can get the privacy key in common with suitable effective detection efficiency and suitable error rate by selecting said threshold values +X ~~and~~ or -X.

Claim 16 (Currently Amended): In quantum cipher communication using a light signal, a quantum cipher communication system ~~having a sender's apparatus, a recipient's apparatus and a transmission path connecting between the sender's apparatus and the recipient's apparatus~~ as set forth in claim15, characterized in that

~~the~~ said sender's apparatus comprises of:

a light source for a laser beam;

a beam splitter for splitting said laser beam into a signal light and a reference light;

a movable mirror making a phase change for every said signal light ; and

a light attenuator for attenuating said signal light intensity,

the transmission path comprises a pair of paths for transmitting said signal light and said reference light respectively,

~~the~~ said recipient's apparatus comprises of:

a movable mirror making a phase change for every said reference light transmitted from the sender's apparatus through one of the path of transmission;

a beam splitter for superimposing said signal light transmitted from the sender's apparatus through the other path of transmission and said reference light phase changed by said movable mirror of the recipient's apparatus;

a pair of photoconductive diodes for converting two output lights from said beam splitter into respective electric signals; and

a charge sensitive amplifier for amplifying a difference signal between said electric signals,

said set of phase changes are 0, 90, 180, and 270 degrees, and

said total phase condition is either 0 or 180 degrees ~~wherein the sender, by using said movable mirror of sender's apparatus, randomly imparts phase changes 0,90,180, or 270 degrees for said every signal light, and the recipient, by using said movable mirror of recipient's apparatus, randomly imparts phase change 0 or 90 degrees for said every reference light, as well~~

~~as measures said difference signal between the electric signals amplified by the charge sensitive amplifier;~~

~~then, by using a public communication line, the recipient notifies to the sender said phase changes imparted by the recipient whether it is 0 or 90 degrees for every reference light;~~

~~the sender calculates the total phase difference between the signal light and the~~ said ~~reference light by adding said phase change notified by the recipient and said phase change imparted~~ made ~~by the sender for every light, and notifies to the recipient the lights whose total phase difference is either 0 or 180 degrees, as a raw key for candidate being adopted as a privacy key;~~

~~then the recipient, for every light notified as a raw key for candidate being adopted as a privacy key, assigns bit 1 when said difference signal measured is equal or greater than a predetermined threshold value +X, and assigns bit 0 when said difference signal measured is equal or less than the predetermined threshold value –X, whereby the recipient gets a privacy key;~~

~~the sender, for every light making notified as a raw key for candidate being adopted as a privacy key, assigns bit 1 when the phase imparted by the sender is 0 or 90 degrees, and assigns bit 0 when the phase imparted by the sender is 180 or 270 degrees, whereby the sender gets the privacy key; and~~

~~wherein the sender and the recipient can get the privacy key in common with suitable effective detection efficiency and suitable error rate by selecting said threshold value +X and –X.~~

Claim 17 (Currently Amended): In quantum cipher communication using a light signal, a quantum cipher communication system ~~having a sender's apparatus, a recipient's apparatus and a transmission path connecting between the sender's apparatus and the recipient's apparatus~~ as set forth in claim15, characterized in that

~~the~~ said sender's apparatus comprises of:

a light source for a linearly polarized pulsed light;

a beam splitter for splitting said linearly polarized pulsed light into a signal light and a reference light;

a first long optical path comprising a half wave plate for rotating the polarization of said signal light by 90 degrees, a light attenuator for attenuating said signal light intensity, a phase modulator for changing the phase of said signal light ~~and mirrors~~; and

a first polarized beam splitter for returning said signal light transmitted through said first long optical path and said reference light onto a common optical axis, wherein said signal light and said reference light returned to the common optical axis have a mutual time delay based on the optical path length difference between said first long

optical path for the signal light and a first short optical path where said reference signal reaches to the first polarized beam splitter from the beam splitter, and have mutually orthogonal polarizations,

the optical fiber comprises a single mode optical fiber connected to said first polarized beam splitter, wherein said signal light and said reference light are transmitted through said single mode optical fiber keeping said time delay and said polarizations,

~~the~~ said recipient's apparatus comprises of:

a second polarized beam splitter for splitting said signal light and said reference light transmitted through the single mode optical fiber;

a second long optical path comprising a half wave plate for rotating the polarization of said reference light and mirrors, and a second short optical path comprising a phase modulator for making a phase change for every signal light transmitted through the single mode fiber, wherein the time delay based on the optical path length difference between said second short optical path and said second long optical path of the recipient's apparatus has the same absolute value and opposite sign to said time delay in the sender's apparatus;

a third polarized beam splitter for superimposing said signal light transmitted through ~~the~~ said second short optical path and said reference light transmitted through ~~the~~ said second long optical path;

a pair of photoconductive diodes for converting two output lights from said third polarized beam splitter into respective electric signals; and

an amplifier for amplifying a difference signal between said electric signals,

said set of phase changes are 0,90,180, and 270 degrees, and

said total phase condition is either 0 or 180 degrees ~~and~~

~~wherein the sender, by using said phase modulation means of sender's apparatus, randomly imparts phase changes 0,90,180, or 270 degrees for every signal light, and the recipient, by using said phase modulation means of recipient's apparatus, randomly imparts phase change 0 or 90 degrees for every reference light, as well as measures said difference signal between the electric signals amplified by the amplifying means;~~

~~then, by using a public communication line, the recipient notifies to the sender said phase changes imparted by the recipient whether it is 0 or 90 degrees for every reference light;~~

~~the sender calculates the total phase difference between the signal light and the reference light by adding said phase change notified by the recipient and said phase change imparted by the sender for every light, and notifies to the recipient the lights whose total phase difference is either 0 or 180 degrees, as a raw key for candidate for being adopted as a privacy key;~~

~~then the recipient, for every light notified as a raw key for candidate being adopted as a privacy key, assigns bit 1 when said difference signal measured is equal or greater than a predetermined threshold value +X, and assigns bit 0 when said difference measured is equal or less than the predetermined threshold value - X, whereby the recipient gets a privacy key;~~

~~the sender, for every light making notified as a raw key for candidate being adopted as a privacy key, assigns bit 1 when the phase imparted by the sender is 0 or 90 degrees, and assigns bit 0 when the phase imparted by the sender is 180 or 270 degrees, whereby the sender gets the privacy key, and~~

~~wherein the sender and the recipient can get the privacy key in common with suitable effective detection efficiency and suitable error rate by selecting said threshold value +X and –X.~~

Claim 18 (Currently Amended): A quantum cipher communication system as set forth in claim 17, characterized in that a third light polarizer is provided in an output side of said single mode optical fiber for making a correction for a disturbance of polarization of said reference ~~signal~~ light.

Claim 19 (Currently Amended): A quantum cipher communication system as set forth in any one of claims 15 to 17, characterized in that in addition to the phase modulations designed to transmit privacy keys, such a phase modulation is so imparted as having a value later determined for making a correction for a fluctuation of the difference in optical path between said reference ~~signal~~ light and said ~~transmission~~ signal light which develops by reason of an external cause.

Claim 20 (Previously Presented): A quantum cipher communication system as set forth in any one of claims 15 to17, characterized in that such phase modulations are so imparted as including those for transmitting privacy keys and those with values later determined are randomly repeated.

Claim 21 (Previously Presented): A quantum cipher communication system as set forth in any one of claims 15 to17, characterized in that eavesdropping is detected on the basis of an increase in the error rate of said difference signal.

Claim 22 (Previously Presented): A quantum cipher communication system as set forth in any one of claims 15 to17, characterized in that eavesdropping is detected on the basis of a change in a Wigner distribution function that indicates a quantum mechanical state of said difference signal.

Claim 23 (Currently Amended): A quantum cipher communication system as set forth in any one of claims 15 to 17, characterized in that for said pair of ~~photoconductor~~ photoconductive diodes, use is made of silicon photoconductor diodes when the light has a wave length of 600 nm to 900 nm, and of InGaAs photoconductor diodes when the light has a wave length of 1000 nm to 1500 nm.

Claim 24 (Currently Amended): A quantum cipher communication system as set forth in any one of claims 15 to 17, characterized in that ~~the~~ said signal light has a typical intensity corresponding to a single photon or so, and said reference light has a typical intensity corresponding to photons as large as 10 millions in number.